PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G10L | A2

(11) International Publication Number: WO 98/10412

(43) International Publication Date: 12 March 1998 (12.03.98)

(21) International Application Number: PCT/US97/15943

(22) International Filing Date: 9 September 1997 (09.09.97)

(30) Priority Data:
08/709,584 9 September 1996 (09.09.96) US

(71) Applicant: VOICE CONTROL SYSTEMS, INC. [US/US]; Suite 100, 14140 Midway Road, Dallas, TX 75244 (US).

(72) Inventor: WEIDEMAN, William, E.; 3121 Cieber Drive, Arlington, TX 76016 (US).

(74) Agent: JUDSON, David, H.; Hughes & Luce, L.L.P., Suite 2800, 1717 Main Street, Dallas, TX 75201 (US).

(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SPEECH RECOGNITION AND VERIFICATION SYSTEM ENABLING AUTHORIZED DATA TRANSMISSION OVER NETWORKED COMPUTER SYSTEMS

(57) Abstract

A system and apparatus for using speech recognition and verification to provide secure and authorized data transmissions between networked computer systems are disclosed. The system comprises first and second network computer systems wherein a request for a transaction by user of the first computer system causes the user to be prompted to enter a spoken identifier such as a credit card number, PIN number or password. This spoken identifier is converted from speech data into speech feature data using either a resident software application or a downloaded application from the second computer system. The speech feature data is transmitted to the second computer system wherein speech recognition and verification engines identify the spoken identifier and determine whether or not the user who spoke the identifier is properly associated with the spoken identifier. Upon successful completion of this recognition and verification process, the requested transaction is completed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

SPEECH RECOGNITION AND VERIFICATION SYSTEM ENABLING AUTHORIZED DATA TRANSMISSION OVER NETWORKED COMPUTER SYSTEMS

TECHNICAL FIELD

The present invention relates to secure data transmission, and more particularly to a method and apparatus authorizing data transmission over a computer network environment utilizing a client/server architecture.

BACKGROUND OF THE INVENTION

The current expansion of computer network systems and linked architectures, such as the Internet, have greatly increased the opportunity for carrying out transactions through networked computers. Unfortunately, the performance of transactions via networked computers requires the transmission of sensitive data (credit card numbers, PIN numbers, passwords, etc.) over the communications network interconnecting the computers. A communications network is for the most part a nonsecure transmission environment that is subject to access by unauthorized third parties. An unauthorized party is able to get a hold of sensitive information by unlawfully monitoring computer communications over the communications network. This of course can be greatly damaging to an individual or business. Also, transfer of data over a

communications network does not provide an easy way to ensure a party is authorized to transmit or receive sensitive data.

One current method for providing secure transmission of sensitive data in a computer network environment rely on encryption of the data prior to transmission. Unfortunately, newly devised decryption methods and faster computer systems continually make it easier for unauthorized third parties to crack any encryption code, thus rendering sensitive data vulnerable to unauthorized attack. Once the sensitive data has been decrypted by an unauthorized individual, this party may now use this sensitive data without authorization to make purchases or carry out any number of unauthorized transactions. Since many current encryption methods have no mechanism for verifying the identity of the person submitting the sensitive information, the unauthorized individual may continue their unlawful activities for a substantial period of time.

Other current systems providing authentication require additional hardware be purchased by the user and an authentication card. The user must insert the authentication card into an associated card reader to access sensitive data. If the card is illegally obtained by an unauthorized individual, this person may still access the sensitive data. Thus, a system enabling secure transmission of sensitive data and verification of a sender's identity would greatly

benefit the expanded use of transactions occurring over networked computer systems.

BRIEF SUMMARY OF THE INVENTION

The present invention overcomes the foregoing and other problems with a system and method using a speech recognition and verification to enable secure data transmissions between networked computer systems. The preferred embodiment of this invention utilizes a client/server architecture wherein a request for a particular transaction by a user at the client unit causes the server unit to prompt the user for a spoken identifier, such as a credit card number, PIN number, password, etc. The user speaks an identifier into a microphone connected to the client unit and the spoken data comprising the identifier is converted into speech feature data. This conversion is carried out by a locally resident software application or may be done by an application or plug-in applet that has been downloaded from the server unit in response to the requested transaction.

The speech feature data is transmitted over a computer communications link from the client unit to the server unit for further processing. Optionally, the speech feature data may be secured by additional state of the art processes, such as encryption, before transmission of the speech feature data to the server unit. A speech recognition engine located at the server unit uses the speech feature data to identify and confirm the spoken identifier entered by the user.

The speech feature data is then further processed by a speech verification engine to confirm that the user who entered the spoken identifier is in fact the user associated with the spoken identifier and is authorized to perform a requested transaction.

Additionally, the speech feature data for the identifier may be compared to previously transmitted versions of the speech feature data for the identifier to determine if it matches any of the previously transmitted versions. When an exact match exists, the transmitted speech feature data is marked as suspect so that further approval steps may be taken. If the spoken identifier is recognized and verified as being associated with the user entering the identifier and no questions arise due to an exact match with previously transmitted data, the transaction request is completed.

The foregoing has outlined some of the more pertinent aspects of the present invention. These aspects should be construed to be merely illustrative of some of the more prominent features and applications of the invention. Many other beneficial results can be attained by applying the disclosed invention in a different manner of modifying the invention as will be described. Accordingly, other aspects and a fuller understanding of the invention may be had by referring to the following Detailed Description of the preferred embodiment.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference should be made to the following Detailed Description taken in connection with the accompanying drawings in which:

FIGURE 1 is a block diagram illustrating the environment of operation of the present invention;

FIGURES 2a and 2b are flow diagrams illustrating the method for providing secure communications;

FIGURE 3 is a flow diagram of the speech recognition and verification algorithms; and

FIGURES 4a and 4b illustrate manners of use for the system of the present invention.

DETAILED DESCRIPTION

Referring now to the drawings and more particularly toFIGURE 1, there is illustrated the general operating environment of the present invention. The preferred embodiment is described with respect to a client/server architecture. A client unit 10 requests a particular transaction or service from the server unit 12 via a networked computer connection 14, such as the Internet. The

server unit 12 includes speech recognition and verification engines 22 which will be more fully discussed in a moment. The client and server units may comprise standalone computers or computer systems.

The client unit 10 includes a network browser 16, in the case of an Internet connection a web browser, and microphone 18. The network browser 16 enables a user to navigate between computers of the interlinked computer network while the microphone 18 enables entry of spoken identifiers at the client unit 10. A speech feature application 20 enables for the conversion of speech data to speech feature data for transmission over the computer network to the speech recognition and verification engines 22 of the server unit 12. The speech feature application 20 may be a plug-in applet, application or helper application that may be downloaded over the computer network to enable the conversion of speech data to speech feature data or may be a software application resident within the client unit 10. While FIGURE 1 illustrates the speech feature application as operating within the network browser 16, it should be appreciated that a helper application operating externally of the browser may be used.

Referring now also to FIGURES 2a and 2b, there are illustrated two flow charts describing the general method of operation of the

present invention. FIGURE 2a illustrates a method wherein recognition of the identifier is confirmed before transmission to the local server while FIGURE 2b illustrates a method wherein confirmation of the recognition is performed at the remote server. The FIGURES 2a and 2b will be described together with similar steps having the same reference numerals. Initially, a user at the client unit 10 makes a transaction request at step 24 to initiate the procedure. The transactions may include a purchase, request for restricted data, etc. The request for a transaction initiates access at step 26 to the speech feature application 20. This access may entail merely opening a resident application on the client unit 10 or automatically downloading an application, helper application or plug-in applet over the Internet connection 14.

Once the speech feature application 20 is ready, the user is prompted to speak a key phrase or identifier at step 28. This phrase may be a credit card number, expiration date, account number, personal identification number or a password. The speech feature application 20 transforms at step 30 the speech data representing the phrase from the microphone 18 into speech feature data used for recognition and verification by the speech recognition and verification engines 22. Conversion of the speech data to speech feature data prior to transmission over the networked computer connection 14 is

desirable due to the fact that a number of bits necessary to represent speech features are smaller than the number of bits necessary to represent the speech itself. However, it should be noted that the speech data may be transmitted to the server unit 12 such that transformation, recognition and verification all occur at the server unit.

In the embodiment of FIGURE 2a, the transformed speech data may be initially recognized at optional step 31 to confirm that the identifier can be correctly identified by the speech recognizer prior to transmission of the data. This step would use a speech recognition algorithm as will be more fully described in a moment. If the data is properly recognized at step 31, control passes off to optional step 32 for further processing of the speech feature data. Otherwise, the user is prompted to reenter the phase or identifier at step 28.

Referring back to both FIGURES 2a and 2b, in an optional step, the speech feature data may be encrypted at step 32 to provide an additional level of security during the transmission process. More security may be obtained by layering additional levels of security on top of the encryption. The order of the transmitted data may also be scrambled to provide an additional layer of encryption. The encrypted data is then transferred at step 34 to the server unit 12 wherein the speech recognition and verification engines 22 are used

to recognize the transmitted information and verify the user transmitting the information at step 38 has the authority to request a transaction using the spoken identifier.

In the alternative embodiment of FIGURE 2b, a determination is made at step 39 whether or not the spoken identifier has been correctly recognized by the recognition algorithm. This may be done in a variety of ways including asking the user to repeat the spoken identifier if a predetermined certainty level of recognition is not achieved or by preparing speech feature data for the transmission back to the client unit and then having this speech feature data processed by the client unit to generate a message indicating the recognized spoken identifier.

Referring again to FIGURES 2a and 2b, once a positive speaker recognition and verification is achieved, the additional procedure of comparing at step 40 the speech featured data for the current transmission against previous transmissions of speech feature data for the same identifier enables a determination of whether or not an exact match exists with a previous transmission. Any exact matches are marked as suspect and routed to the server unit 12 for appropriate action. This process relies on the fact that speech features from one utterance to the next will be slightly different each time the utterance is spoken by the user. Comparison of the

utterance to previous transmissions prevents an unauthorized user from intercepting a previous transmission and merely recording and replaying the information to achieve unauthorized access. If the transmitted information and the identity of the user are verified, the transaction is confirmed at step 42 and the transaction is completed.

Referring now to FIGURE 3, a block diagram is shown of an embodiment of the voice recognition and verification algorithms 48 and 50. The functional blocks set forth in the upper portion of the block diagram comprise those steps which are performed by the speech feature application 20 located at the client unit 10. These blocks comprise speech processing means for carrying out a first tier of a multistage data reduction process. In particular, as speech is input to the speech feature application 20, a feature extractor 60 extracts a set of primary features that are computed in real time every 10 milliseconds. The primary features include heuristically-developed time domain features (e.g. zero crossing rates) and frequency domain information such as fast fourier transform (FFT) coefficients. The output of the feature extractor 60 is a reduced set (approximately 40,000 data points/utterance instead of the original approximately 80,000 data points/utterance) and is applied to a trigger routine 62 that captures spoken words using the primary features. The trigger routine 62 is connected to a secondary feature

routine 63 for computing "secondary features" from the primary features. The secondary features preferably result from non-linear transformations of the primary features. The output of the routine 63 is connected to phonetic segmentation routine 64. After an utterance is captured and the secondary features are computed, the routine 64 provides automatic phonetic segmentation. To achieve segmentation, the phonetic segmentation routine 64 preferably locates voicing boundaries by determining an optimum state sequence of a two-state Markov process based on a sequence of scalar discriminate function values. The discriminate function values are generated by a two-class Fisher linear transformation of secondary feature vectors. The voicing boundaries are then used as anchor points for subsequent phonetic segmentation.

After the phonetic boundaries are located by the phonetic segmentation routine, the individual phonetic units of the utterance are analyzed and so called "tertiary features" are computed by a tertiary feature calculation routine 64. These tertiary features preferably comprise information (e.g., means or variances) derived from the secondary features within the phonetic boundaries. The tertiary features are used by both the voice recognition algorithm 48 and the voice verification algorithm 50 as will be described. The output of the routine 65 is a tertiary feature vector of approximately

300 data points/utterance. As can be seen then, the upper portion of FIGURE 3 represents the first tier of the multistage data reduction process which significantly reduces the amount of data to be analyzed and transferred over the Internet connection 14 that still preserves the necessary class of separability, whether it is digit-relative or speaker-relative, necessary to achieve recognition or verification, respectively. The middle portion of FIGURE 3 represents a second tier of the data reduction process, and as will be described, comprises the transformation routines 49a and 49b occurring at the voice verification and recognition engines 22 of the server unit 12.

To effect speaker independent voice recognition, the tertiary features are first supplied to the voice recognition linear transformation routine 49a. This routine multiplies the tertiary feature vector by the voice recognition feature transformation data (which is a matrix) 52a to generate a voice recognition parameter data factor for each digit. The output of the transformation routine 49a is then applied to a voice recognition statistical decision routine 66a for comparison with the voice recognition class of reference data 52b. The output of the decision routine 66a is a yes/no decision identifying whether the digit is recognized and, if so, which digit was spoken.

Specifically, a decision routine 66a evaluates a measure of word similarity for each of the eleven digits (zero thorough 9 and "OH") in the vocabulary. The voice recognition class reference data 52b includes various elements (e.g., acceptance thresholds for each digit class, inverse covariances and mean vectors for each class) used by the decision strategy. For a digit to be declared (as opposed to being rejected), certain acceptance criteria must be met. The acceptance criteria may include, but need not be limited to the following: The voice recognition algorithm determines the closest match between the class reference data and the voice recognition parameter vector for the digit; this closest match is a so-called "first choice." The next closest match is a "second choice." Each choice has its own matching score. The digit is declared if (1) the matching score of the first choice is below a predetermined threshold, and (2) the difference between the matching scores of the first choice and the second choice digits is greater than another predetermined threshold. When all words of the spoken identifier have been recognized, the voice recognition portion of the method is complete.

To effect voice verification, the tertiary features are also supplied to a linear transformation routine 49b that multiples each tertiary feature vector by the voice verification feature transformation data (which is a matrix). The output of the routine 49b is an N

element vector of voice verification parameter data for each digit of the password, with N preferably approximately equal to 25. The voice verification parameter data vector is then input to a verifier routine 66b which also receives the voice verification class reference data for the caller. Specifically, the voice verification class reference data is provided from the voice verification reference database 55. As noted above, the address in the database 55 of the user's voice verification class reference data is defined by the user's password derived by the voice recognition algorithm 48.

Verifier routine 66b generates one of three different outputs: ACCEPT, REJECT and TEST. An ACCEPT output may authorize the user to access data from the transaction database 56. The REJECT output is provided if the verifier disputes the purported identify of the user. The TEST output initiates the prompting step wherein additional follow-up questions are asked to verify the user's identity.

Referring now to FIGURES 4a and 4b, there are illustrated alternative embodiments of the present invention wherein the speech recognition and speech verification engine software is distributed. In FIGURE 4a, a customer 90 speaks an identifier which is transformed into speech feature data and transmitted to the merchant server 94. The merchant server 94 runs the speech features through the recognition engine software 96 to recognize the identifier provided by

the customer 90. The customer is queried once the spoken identifier is recognized to confirm it has been correctly identified. Once confirmed, the recognized identifier, the features for speech verification and the transaction data are sent to the payment gateway processor server 98 for verification, using speech verification engine software 100, of the authorization of the customer providing the spoken identifier to carry out a requested transaction. Once the identifier is verified, the payment gateway processor server 98 transmits authorization to complete the transaction to the merchant server. Transmissions preferably occur over a secure channel such as a dedicated phone line or dedicated computer network between the payment gateway processor server 98 and the merchant server 94. Once the merchant server 94 obtains a successful authorization, the merchant completes the transaction with the customer and delivers the product or services.

FIGURE 4b illustrates another method wherein the merchant server 94 simply passes the speech feature data and transaction data to the payment gateway processor server 98 so that recognition and verification are both accomplished by software engines 102 at the payment gateway processor server 98. This method may be used to limit the possibility of merchant fraud. The payment gateway processor server 98 confirms recognition with the customer and

determines the required response to the credit authorization requests and notifies the merchant of the results. Upon recognition and verification of authority to perform the transaction, transaction approval is transmitted to the merchant server 94.

Use of the embodiments illustrated in FIGURES 4a and 4b may occur in the manner of a user speaking their credit card authorization number into a terminal or unit located at a merchant location. Alternatively, the user may enter their credit card number via a magnetic card reader terminal or key pad entry and speak an identifier such as their name that does not reveal any secret to an eavesdropper.

It should be appreciated by those skilled in the art that the specific embodiments disclosed above may be readily utilized as a basis for modifying or designing other structures for carrying out the purpose of the present invention. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the spirit and scope of the invention as set forth in the appended claims.

CLAIMS

What is claimed is:

1. A system for providing secure data transmissions between networked computer systems, comprising:

a server system connected to a plurality of client systems through a computer communications link for receiving transaction requests and speech feature data from the client system;

means within the server system for prompting the client system to request a spoken identifier from the client system in response to the transaction request;

a recognition engine within the server system for recognizing the spoken identifier represented by the speech feature data received from the client system;

a verification engine within the server system for verifying the spoken identifier represented by the speech feature data is associated with a user speaking the identifier; and

means for completing the transaction request upon verification of the association of the user with the spoken identifier.

2. The system of Claim 1 further including means for automatically transferring a speech feature extraction engine to the client system in response to the transaction request.

3. The system of Claim 1 wherein the recognition engine further includes means for confirming a spoken identifier has been correctly identified.

4. The system of Claim 3 wherein the means for confirming actuates the means for prompting to request reentry of the spoken identifier if the spoken identifier is not recognized.

5. The system of Claim 1 wherein the computer communications link comprises the Internet.

6. The system of Claim 1 wherein the verification engine further includes means for determining if the received speech feature data matches previously received speech feature data.

7. The system of Claim 1 further including means for decrypting speech feature data received from the client system.

8. A method for securely transmitting data between computer systems on a computer communications link, comprising the steps of:

prompting a user at a first computer system to enter a spoken identifier in response to a transaction request by the user;

converting the spoken identifier from speech data to speech feature data using a speech transformation engine;

transmitting the speech feature data to a second computer system;

identifying the spoken identifier using a speech recognition engine;

verifying the spoken identifier was entered by a user associated with the spoken identifier using a speech verification engine; and

providing the requested transaction if the identified spoken identifier was spoken by the associated user.

9. The method of Claim 8 further including the step of confirming the spoken identifier was correctly identified by the speech recognition engine.

10. The method of Claim 9 further including the step of re-prompting the user to enter a spoken identifier if the spoken identifier is not correctly identified.

11. The method of Claim 8 further including the step of transferring a speech feature extraction engine to the first computer system in response to the transaction request.

12. The method of Claim 8 further including the steps of:

comparing the speech feature data received from the first computer system to previously received speech feature data to determine if any identical matches exist; and

identifying the speech feature data as suspect if the received speech feature data exactly matches previously received speech feature data.

13. The method of claim 8 further including the step of encrypting the speech feature data prior to transmission to the second computer system.

14. The method of Claim 11 further including the step of decrypting the speech feature data prior to identifying the spoken identifier.

15. The method of Claim 8 further including the step of prompting the user at the first computer system to enter a first

identifier containing sensitive information and wherein the spoken identifier comprises verifying information.

16. A method for securely transmitting between computer systems on a computer communications link, comprising the steps of:

prompting a user at a first computer system to speak a character string beginning with a first character and ending with a last character thereof in response to a transaction request by the user;

generating speech feature data for each spoken character of the character string;

transmitting the speech feature data to a second computer system over the computer communications link;

applying the speech feature data of the character string and voice recognition transformation data to a voice recognition feature transformation to generate a first set of parameters for each spoken character of the first character string, the first set of parameters for use in a voice recognition system;

applying the speech feature data and voice verification feature transformation data to a voice verification feature transformation to generate a second set of parameters for each

spoken character of the first character string, the second set of parameters for use in a voice verification system;

recognizing the character string using the first set of parameters;

verifying the user is associated with the character string using the second set of parameters; and

providing the requested transaction over the computer communications link if the user is verified and the character string is recognized.

17. The method of Claim 16 further including the step of transferring a speech feature extraction engine to the first computer system in response to the transaction request.

18. The method of Claim 16 wherein the step of verifying further includes the steps of:

comparing the speech feature data received from the first computer system to previously received speech feature data to determine if any identical matches exist; and

identifying the received speech feature data as suspect if the speech feature data exactly matches previously received speech feature data.

19. The method of claim 16 further including the step of encrypting the speech feature data prior to transmission to the second computer system.

5

20. The system of Claim 19 further including the step of decrypting the speech feature data prior to identifying the spoken identifier.

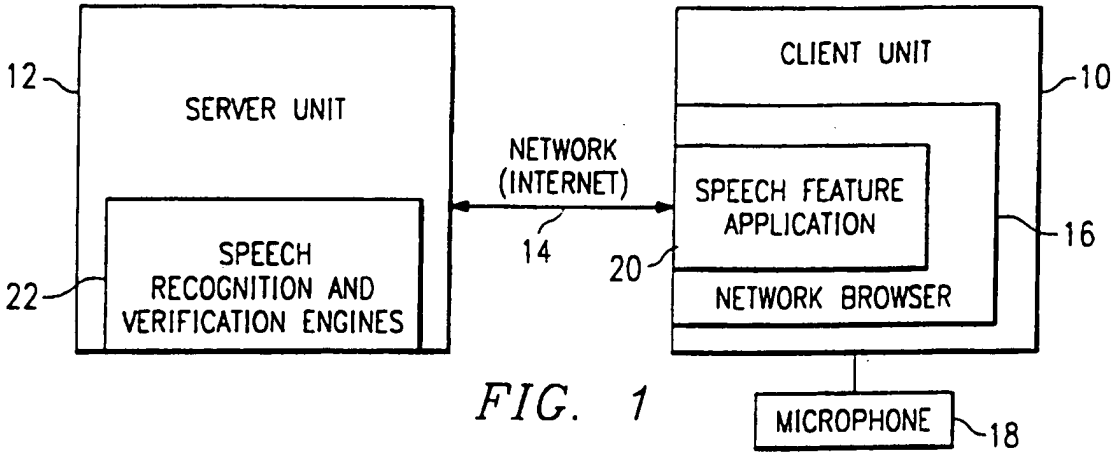


FIG. 1

FIG. 2a

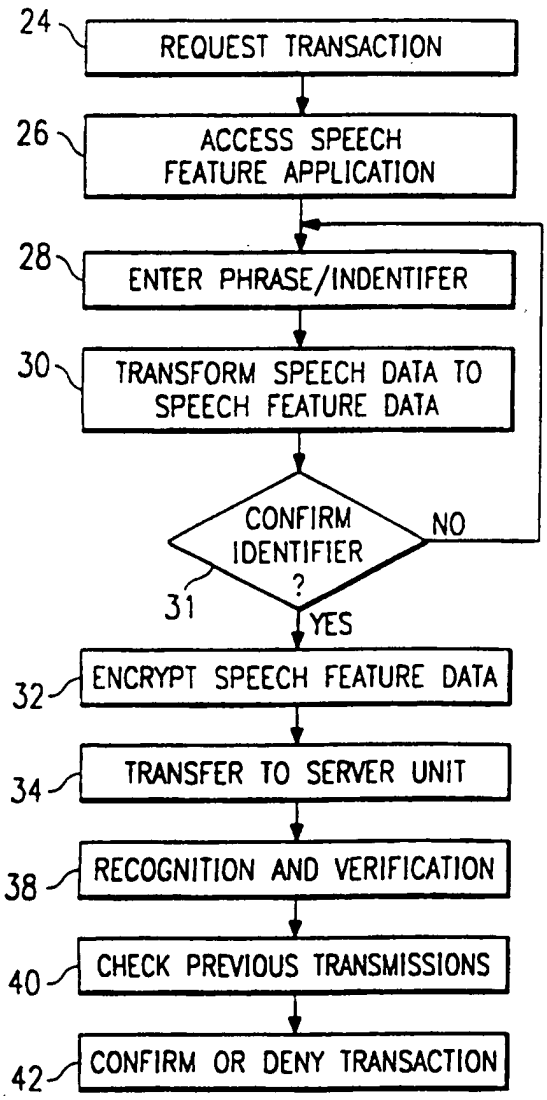
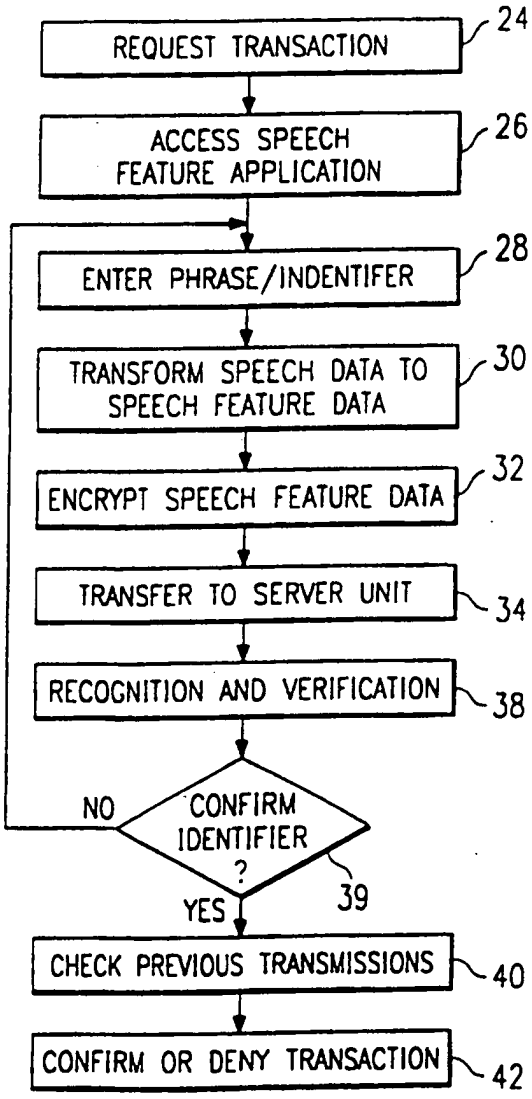


FIG. 2b



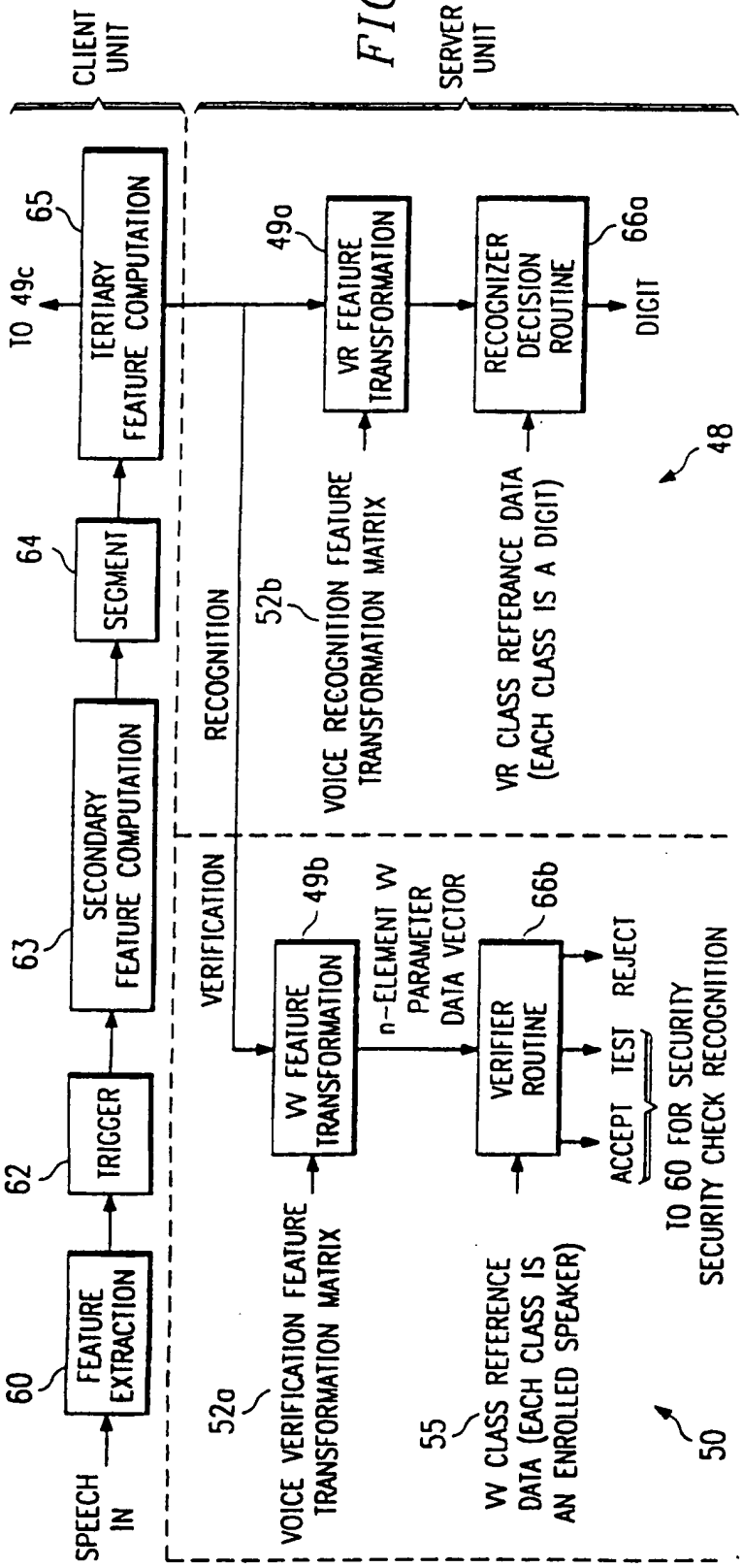


FIG. 3

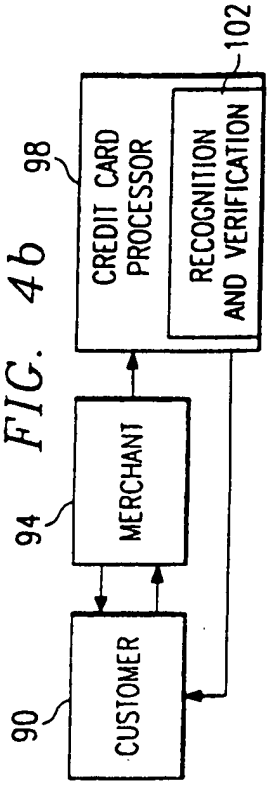


FIG. 4b

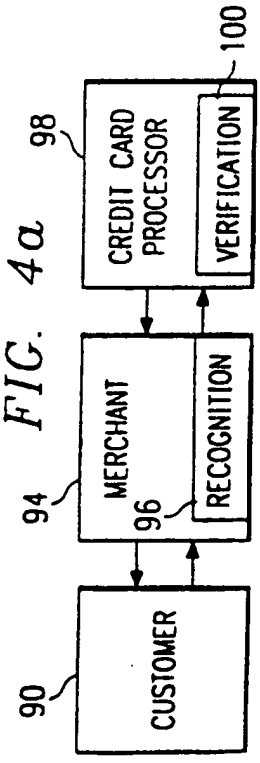


FIG. 4a

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G10L 5/06

A3

(11) International Publication Number: WO 98/10412

(43) International Publication Date: 12 March 1998 (12.03.98)

(21) International Application Number: PCT/US97/15943

(22) International Filing Date: 9 September 1997 (09.09.97)

(30) Priority Data:
08/709,584 9 September 1996 (09.09.96) US

(71) Applicant: VOICE CONTROL SYSTEMS, INC. [US/US]; Suite 100, 14140 Midway Road, Dallas, TX 75244 (US).

(72) Inventor: WEIDEMAN, William, E.; 3121 Cieber Drive, Arlington, TX 76016 (US).

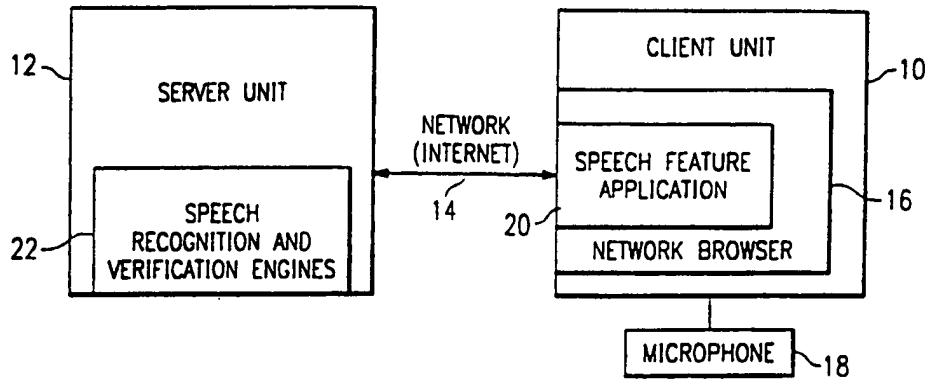
(74) Agent: JUDSON, David, H.; Hughes & Luce, L.L.P., Suite 2800, 1717 Main Street, Dallas, TX 75201 (US).

(81) Designated States: AU, CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(88) Date of publication of the international search report:
9 July 1998 (09.07.98)

(54) Title: SPEECH VERIFICATION SYSTEM AND SECURE DATA TRANSMISSION



(57) Abstract

A system and apparatus using speech recognition and verification (22) to provide secure and authorized data transmission between networked computer systems are disclosed. The system comprises first and second network computer systems wherein a request for a transaction by user of the first computer system causes the user to be prompted to enter a spoken identifier such as a credit card number, PIN number or password. This spoken identifier is converted from speech data into speech feature data using either a resident software application or a downloaded application from the second computer system. The speech feature data is transmitted to the second computer system wherein speech recognition and verification engines identify the spoken identifier and determine whether or not the user who spoke the identifier is properly associated with the spoken identifier. Upon successful completion of this recognition and verification process, the requested transaction is completed.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/15943

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G10L 5/06
US CL :704/273

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 704/273, 231, 243, 270, 275; 379/88' 380/23

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN (Inspec, Japio, wpids)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,297,194 A (HUNT ET AL) 22 March 1994, Fig. 2, Blocks 52a to 52 c, Abstract, lines 7-9.	1-20
Y	US 5,517,558 A (SCHALK) 14 May 1996, Abstract.	1-20
A	US 5,343,529 A (GOLDFINE ET AL) 30 August 1994, Fig. 1.	1-20
A,P	US 5,610,981 A (MOONEY ET AL) 11 March 1997, see Abstarct.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 11 FEBRUARY 1998	Date of mailing of the international search report 09 MAR 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer RICHEMOND DORVIL Telephone No. (703) 305-9645

Form PCT/ISA/210 (second sheet)(July 1992)*